

Web Gateway Cloud Service IPSec Configuration

Juniper SSG5 Example - NetScreen 6.3.0r21.0

(Firewall+VPN)

This document describes configuration of the Juniper SSG5 device running NetScreen OS. The tested NetScreen version was 6.3, but we expect the configuration to work with other versions and appliances running similar OS. Key capabilities are IPSec Gateway to Gateway VPN supporting IKEv2 and Policy Based routing for any destination (0.0.0.0/0).

All configuration assumes that the firewall is already set up for basic routing:

- Ethernet0/0 is configured in the Untrust zone, and bgroup0 is configured in the Trust zone.
- McAfee Web Gateway Cloud Service (McAfee WGCS) is configured with a pre-shared secret, your external public IP, and the local subnet where client web traffic is sourced.

Basic Steps

1. Configure Tunnel Interfaces
2. Configure VPNs and Bind to Tunnel Interfaces
3. Create Policy Based Routing (PBR) Policy
4. Bind PBR Policy to Client Interface(s)

Configure Tunnel Interfaces

From **Network > Interfaces > List**, add two new tunnel interfaces to the Untrust zone.

- **Zone (VR)** – Untrust (trust-vr)
- **Unnumbered** – Selected
- **Interface** – ethernet0/0 (trust-vr)
- **Maximum Transfer Unit(MTU)** – 1300

Tunnel Interface Name tunnel.1

Zone (VR) Untrust (trust-vr) ▼

Fixed IP

IP Address / Netmask 0.0.0.0 / 0

Unnumbered

Interface ethernet0/0 (trust-vr) ▼

Maximum Transfer Unit(MTU) Admin MTU 1300 Bytes (Operating MTU: 1300; Default MTU: 1500)

DNS Proxy

Network > Interfaces (List) ssg5-serial ?

List 20 per page

List ALL(10) Interfaces New Tunnel IF ▼

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure	
bgroup0	192.168.10.1/24	Trust	Layer3	Up	-	Edit	
ethernet0/2				Up	-	Edit	
ethernet0/3				Up	-	Edit	
ethernet0/4				Up	-	Edit	
ethernet0/5				Down	-	Edit	
ethernet0/6				Down	-	Edit	
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit	
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit	
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit	
ethernet0/0	68.49.53.191/23	Untrust	Layer3	Up	-	Edit	
ethernet0/1	192.168.111.0/24	DMZ	Layer3	Down	-	Edit	
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit	
tunnel.1	unnumbered	Untrust	Tunnel	Down	-	Edit	Remove
tunnel.2	unnumbered	Untrust	Tunnel	Down	-	Edit	Remove
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit	

Configure VPNs and Bind to Tunnel Interfaces

From **VPNs > AutoKey Advanced > P1 Proposal**, create a custom Phase One Proposal.

- **Name** – WGCSP1 (example)
- **Authentication Method** – Preshare
- **DH Group** – Group 5
- **Encryption Algorithm** – AES-CBC(128 Bits)
- **Hash Algorithm** – SHA2_256
- **Lifetime** – 28800 (Sec)

VPNs > AutoKey Advanced > P1 Proposal > Edit sbg5-serial ?

Juniper
NETWORKS

SSG5-Serial

- Home
- Configuration
- Network
 - Binding
 - DNS
 - Zones
- Interfaces
 - List
 - Backup
- DHCP
- 802.1X
- Routing
- PPP
- DSCP
- Security
- Policy
- VPNs
 - AutoKey IKE
 - AutoKey Advanced
 - Gateway
 - P1 Proposal
 - P2 Proposal

Name:

Authentication Method:

DH Group:

Encryption & Data Integrity

Encryption Algorithm:

Hash Algorithm:

Lifetime:

Sec Min Hours Days

VPNs > AutoKey Advanced > P1 Proposal sbg5-serial ?

List per page Go to page

Name	Method	DH group	Encrypt/Auth	Life Time	Configure
WGCSP1	Preshare	5	AES128/SHA2-256	28800	Edit

From **VPNs > AutoKey Advanced > P2 Proposal**, create a custom Phase Two Proposal.

- **Name** – WGCSP2 (example)
- **Perfect Forward Secrecy** – DH Group 5
- **Encryption (ESP)** – Selected
- **Encryption Algorithm** – AES-CBC(128 Bits)
- **Authentication Algorithm** – SHA2_256
- **Lifetime** – 28800 (Sec)

Name

Perfect Forward Secrecy

Encapsulation

Encryption (ESP)

Encryption Algorithm

Authentication Algorithm

Authentication Only (AH)

Authentication Algorithm

Lifetime

In Time

Sec Min Hours Days

In Kbytes Kbytes

VPNs > AutoKey Advanced > P2 Proposal ssg5-serial ?

List 20 per page New

Name	PFS	Encap.	Encrypt/Auth	Life Time	Life Size	Configure
nopfs-esp-des-md5	No PFS	ESP	DES/MD5	3600	0	
nopfs-esp-des-sha	No PFS	ESP	DES/SHA-1	3600	0	
g2-esp-des-md5	DH Group 2	ESP	DES/MD5	3600	0	
g2-esp-des-sha	DH Group 2	ESP	DES/SHA-1	3600	0	
nopfs-esp-3des-md5	No PFS	ESP	3DES/MD5	3600	0	
nopfs-esp-aes128-md5	No PFS	ESP	AES128/MD5	3600	0	
g2-esp-3des-md5	DH Group 2	ESP	3DES/MD5	3600	0	
g2-esp-aes128-md5	DH Group 2	ESP	AES128/MD5	3600	0	
nopfs-esp-3des-sha	No PFS	ESP	3DES/SHA-1	3600	0	
g2-esp-3des-sha	DH Group 2	ESP	3DES/SHA-1	3600	0	
nopfs-esp-aes128-sha	No PFS	ESP	AES128/SHA-1	3600	0	
g2-esp-aes128-sha	DH Group 2	ESP	AES128/SHA-1	3600	0	
WGCS2	DH Group 5	ESP	AES128/SHA2-256	28800	0	Edit

Create two VPN Gateway definitions – When you repeat this procedure for the second Gateway, assign a different name and static IP address.

From **VPNs > AutoKey Advanced > Gateway**, configure these settings.

- **Gateway Name** – WGCS1 or WGCS2 (examples)
- **Version** – IKEv2
- **Remote Gateway** – Selected

- **Static IP Address** – Specify the resolved IP address for each gateway from a DNS lookup of 1.network.c<customerid>.saasprotection.com or 2.network.c<customerid>.saasprotection.com.
- **IKEv2 Auth Method** – Selected
- **Self** – preshare
- **Peer** – preshare
- **Preshared Key** – Must match the value configured in McAfee WGCS
- **Security Level** – Select **User Defined** (Custom).
- **Phase 1 Proposal** – Select WGCSP1, None, None, None.
- **Enable NAT-Traversal** – Selected

Gateway Name

Version IKEv1 IKEv2

Remote Gateway

Static IP Address IP Address/Hostname

Dynamic IP Address Peer ID

Dialup User User

Dialup User Group Group

ACVPN-Dynamic

Local ID

ACVPN-Profile

Click **Advanced** to open more settings.

IKEv2 Auth Method

Self: preshare ▼
Peer: preshare ▼

Preshared Key: Use As Seed

Local ID: (optional)

Outgoing Interface: ethernet0/0

Security Level

Predefined: Standard Compatible Basic

User Defined: Custom

Phase 1 Proposal

WGCS1 ▼ None ▼ None ▼ None ▼

Mode (Initiator): Main (ID Protection) Aggressive

Enable NAT-Traversal

UDP Checksum:

Keepalive Frequency: 0 Seconds (0~300)

Peer Status Detection

Heartbeat

Hello: 0 Seconds (1~3600, 0: disable)

VPNs > AutoKey Advanced > Gateway ssg5-serial ?

List 20 per page New

Name	Peer Type	Address/ID/User Group	Local ID	Security Level	Configure	
WGCS1	Static	185.125.226.1	-	Custom	Edit	EAP/MODECFG -
WGCS2	Static	185.125.226.2	-	Custom	Edit	EAP/MODECFG -

Create a VPN tunnel binding for two tunnel interfaces – When you repeat this procedure for the second interface (tunnel. 2), assign the VPN binding a different name, such as WGCSVPN2.

From **VPNs > AutoKey IKE**, configure these settings.

- **VPN Name** – WGCSVPN1 or WGCSVPN2 (examples)
- **Remote Gateway** – Selected
- **Predefined** – WGCS1
- **Security Level** – Select **User Defined (Custom)**.
- **Phase 2 Proposal** – Select WGCS2, None, None, None.
- **Bind to** – Select **Tunnel Interface**, tunnel.1.

VPN Name

Remote Gateway
 Predefined WGCS1 ▾
 Create a Simple Gateway

Gateway Name

Version IKEv1 IKEv2

Type Static IP Address/Hostname

Dynamic IP Peer ID

Dialup User User None ▾

Dialup Group Group None ▾

Local ID (optional)

Preshared Key Use As Seed

Security Level Standard Compatible Basic

Outgoing Interface ethernet0/0 ▾

ACVPN-Dynamic
 ACVPN-Profile

Gateway None ▾
 Tunnel Towards Hub None ▾

Binding to Tunnel None ▾

Click **Advanced** to open more settings.

Security Level

Predefined Standard Compatible Basic
 User Defined Custom

Phase 2 Proposal

WGCS2 ▾
None ▾
None ▾
None ▾

Replay Protection
 Transport Mode

Bind to None
 Tunnel Interface tunnel.1 ▾
 Tunnel Zone Untrust-Tun ▾

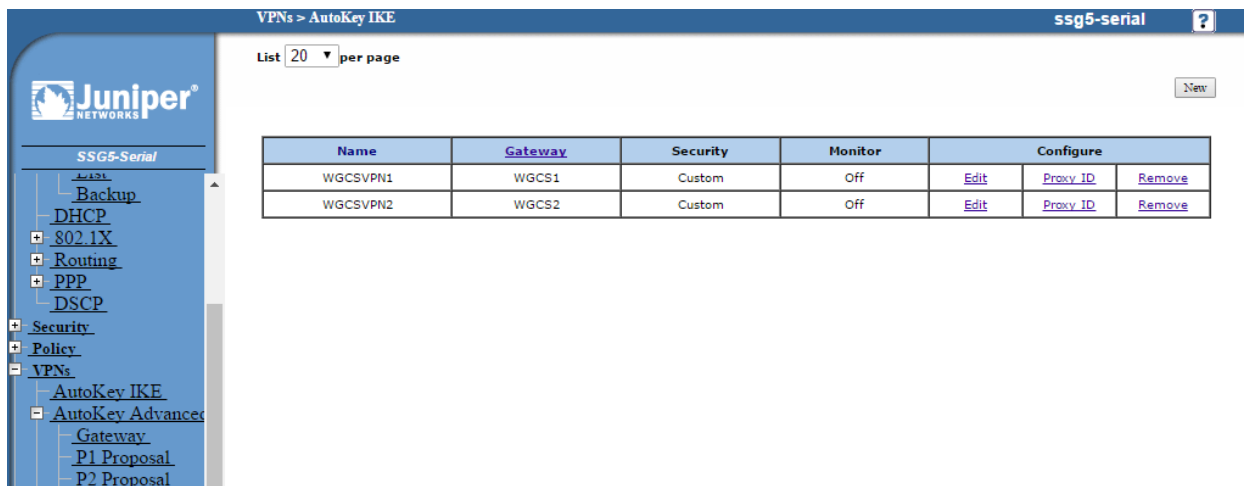
Proxy-ID Check

DSCP Marking Disable
 Enable
 Dscp Value

VPN Group None ▾
Weight

VPN Monitor
 Source Interface default ▾
 Destination IP

Optimized
 Rekey

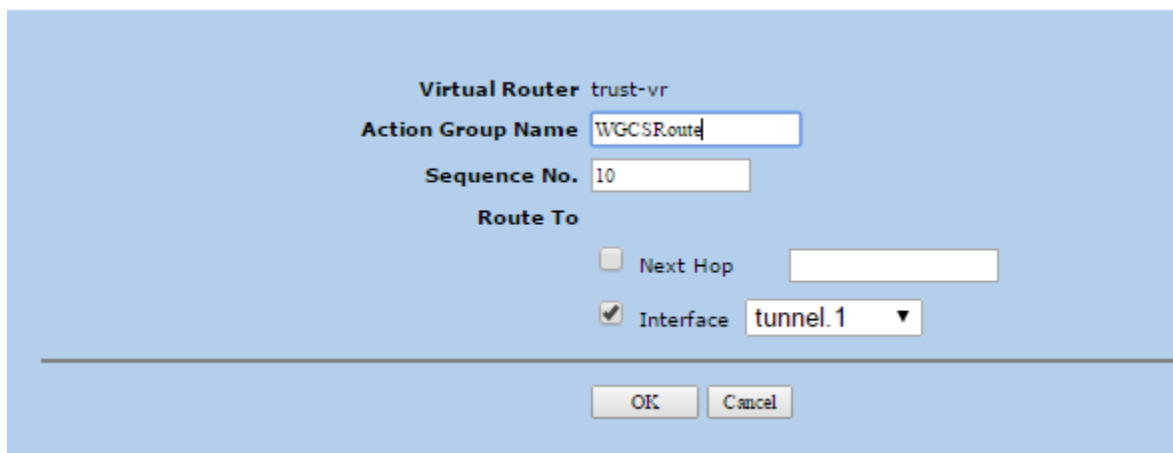


Create Policy Based Routing (PBR) Policy

Create an Action Group with two routes – When you repeat this procedure for the second route, use 20 for the sequence number and tunnel.2 for the interface.

From **Network > Routing > PBR > Action Group**, configure these settings.

- **Virtual Router** – trust-vr
- **Action Group Name** – WGCSRoute (example)
- **Sequence No.** – 10
- **Route To** – Select **Interface**, tunnel.1.



This screenshot shows an action group named WGCSBypass that when combined with a match group in a policy allows specified traffic to bypass McAfee WGCS.

Network > Routing > PBR > Action Group List ssg5-serial ?

List 20 per page
 Action Group for All virtual routers trust-vr New

trust-vr		
Action Group ID : WGCSRoute		Add Seq No Remove
Seq No	Next Interface/Next Hop	Configure
10	tunnel.1	Remove
20	tunnel.2	Remove
Action Group ID : WGCSBypass		Add Seq No Remove
Seq No	Next Interface/Next Hop	Configure
10	ethernet0/0	Remove

Create an ACL with two entries – When you repeat this procedure for the second entry, use 20 for the sequence number and 443 for the destination port.

From **Network > Routing > PBR > Extended ACL**, configure these settings.

- **Virtual Router** – trust-vr
- **Extended ACL ID** – 1
- **Sequence No.** – 10
- **Destination Port** – 80~80
- **Protocol** – TCP

Virtual Router trust-vr

Extended ACL ID

Sequence No.

Source IP Address / Netmask /

Source Port ~

Destination IP Address / Netmask /

Destination Port ~

Protocol

IP-TOS (1~255)

This screenshot shows that ACL 2 that will allow HTTP/HTTPS traffic from the specified source IP address to bypass McAfee WGCS when used in a match group combined with the WGCSBypass action.

Network > Routing > PBR > Extended ACL List ssg5-serial ?

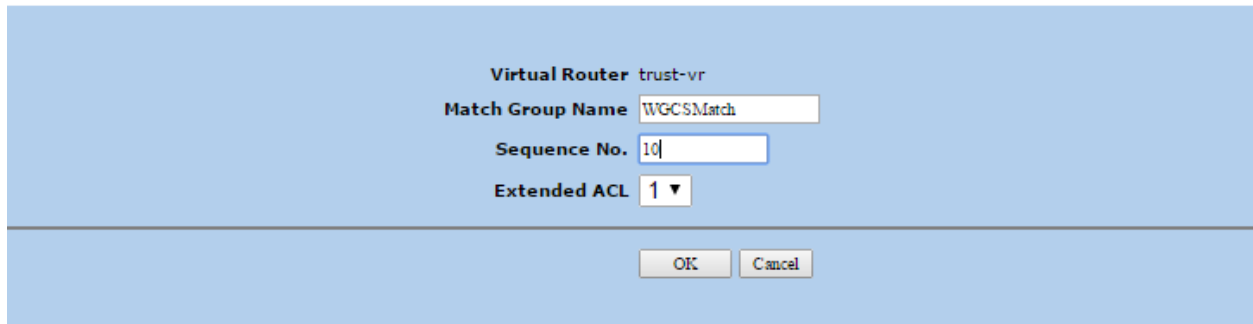
List per page

Extended Access List for

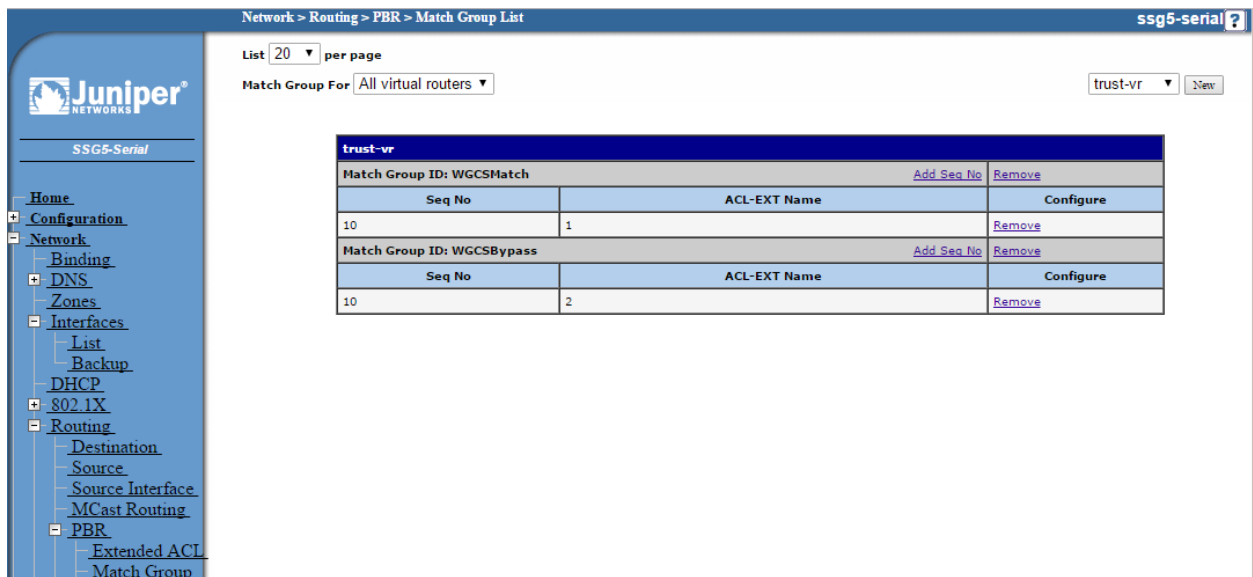
trust-vr							
Extended Access List ID : 1 Add Seq No Remove							
Seq No	Source IP	Source Port	Destination IP	Destination Port	Protocol	QOS Priority	Configure
10	N/A	N/A	N/A	80~80	TCP	N/A	Remove
20	N/A	N/A	N/A	443~443	TCP	N/A	Remove
Extended Access List ID : 2 Add Seq No Remove							
Seq No	Source IP	Source Port	Destination IP	Destination Port	Protocol	QOS Priority	Configure
10	192.168.11.122/32	N/A	N/A	80~80	TCP	N/A	Remove
20	192.168.11.122/32	N/A	N/A	443~443	TCP	N/A	Remove

Create a Match Group – Match groups allow you to associate one or more ACLs with a match group name and ID number.

From **Network > Routing > PBR > Match Group**, configure the settings shown in the screenshot.



This screenshot shows that ACL 2 is associated with the match group name WGCSBypass. Specify this match group when configuring the policy.



Create a Routing Policy for McAfee WGCS – Policies bind match groups and action groups together.

From **Network > Routing > PBR > Policy**, configure the settings shown in the screenshot.

Virtual Router trust-vr

Policy Name

Sequence No.

Match Group

Action Group

OK Cancel

This screenshot shows the WGCSBypass match and action groups combined in sequence number 10 of the policy named WGCSPolicy. This policy allows the HTTP/HTTPS traffic configured in ACL 2 to bypass McAfee WGCS and go directly to the internet as configured in the WGCSBypass action group.

Network > Routing > PBR > Policy List ssg5-serial ?

List per page

Policy List for trust-vr New

trust-vr			
Policy Name: WGCSPolicy Add Seq No Remove			
Policy Name	Match Group	Action Group	Configuration
10	WGCSBypass	WGCSBypass	Remove
20	WGCSMatch	WGCSRoute	Remove

Juniper NETWORKS
SSG5-Serial

- Home
- Configuration
- Network
 - Binding
 - DNS
 - Zones
 - Interfaces
 - List
 - Backup
 - DHCP
 - 802.1X
 - Routing
 - Destination
 - Source
 - Source Interface
 - MCast Routing
 - PBR
 - Extended ACL
 - Match Group
 - Action Group
 - Policy
 - Policy Binding

Bind PBR Policy to Client Interface(s)

Bind WGCSPolicy to the trusted interfaces.

From **Network > Routing > PBR > Policy Binding**, select the N/A hyperlink under **Policy Name** for the client interface in the Trust zone that you want to edit. Configure these settings.

- **Interface** – bgroup0
- **Enable** – Selected

- Policy – WGCSPolicy

Policy Binding

Interface bgroup0

Enable


Policy WGCSPolicy ▼

Network > Routing > PBR > Policy Binding ssg5-serial ?

List 20 per page

Policy Binding List for All virtual routers ▼

Virtual Router	Policy Name	Zone	Policy Name	Interface	Policy Name	Action Policy
trust-vr	N/A	Trust	N/A	bgroup0	WGCSPolicy	WGCSPolicy
		Untrust	N/A	ethernet0/0	N/A	N/A
				tunnel.1	N/A	N/A
		tunnel.2	N/A	N/A		
		DMZ	N/A	ethernet0/1	N/A	N/A



SSG5-Serial

- Home
- Configuration
- Network
 - Binding
 - DNS
 - Zones
 - Interfaces
 - List
 - Backup
 - DHCP
 - 802.1X
 - Routing
 - Destination
 - Source
 - Source Interface
 - MCast Routing
 - PBR
 - Extended ACL
 - Match Group
 - Action Group
 - Policy
 - Policy Binding